

REMARKS

Favorable reconsideration of this application, as presently amended and in light of the present discussion, is respectfully requested.

Claims 1-4, 6-14, 16-19, 21-23, 25, and 26 are pending in this application. Claims 1, 3, 4, 16, 18, 19, 21-23, and 26 are amended by the present amendment.

Amendments to the claims find support in the application as originally filed at least at page 35, lines 15-25, and in Applicants' Fig. 11. Thus, no new matter is added.

In the outstanding Office Action, Claims 1-4, 16-19, 21-23, 25, and 26 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Publication 2002/0012433 to Haverinen et al. (herein "Haverinen") in view of U.S. Patent 7,058,414 to Rofheart et al. (herein "Rofheart") and U.S. Publication 2003/0065918 to Willey; and Claims 6-14 were rejected under 35 U.S.C. § 103(a) as unpatentable over Haverinen and Rofheart.

Applicants respectfully traverse the rejection of Claims 1-4, 16-19, 21-23, 25, and 26 under 35 U.S.C. § 103(a) as unpatentable over Haverinen, Rofheart, and Willey.

Claim 1 is directed to a data transmitting apparatus that includes, in part, a command transmission unit configured to transmit a response request command to a data receiving apparatus, a control unit configured to receive a response message to the response request command from the data receiving apparatus, and an expected value generation unit configured to generate an expected authentication value based on shared data shared with the data receiving apparatus and a sequence number. The sequence number indicates an ordinal position of the response request command in a sequence of response request commands to be transmitted by the command transmission unit.

According to a non-limiting embodiment of a data transmitting apparatus for example as shown in Applicants' Fig. 11, a counter is incremented for each received response, and a sequence number C_j in a response is checked to see if it is equal to a current value of the

counter, for example as in step S58. Further, as noted in Applicants' specification, generation of an expected authentication value based on shared data and a sequence number indicating an ordinal position of a command in a sequence of commands may advantageously make it impossible for a receiving terminal to transmit a response message until after the command is received from the transmitting side terminal. Therefore, it is advantageously possible according to an embodiment of the present invention to prevent an illegal act such as transmitting a response message before a command is received to deceptively shorten a response time.¹

Applicants respectfully submit that Haverinen, Rofheart, and Willey fail to teach or suggest each of the features of independent Claims 1, 3, 4, 16, 18, 19, 21-23, and 26. For example, Applicants respectfully submit that Haverinen, Rofheart, and Willey fail to teach or suggest an expected value generation unit configured to generate an expected authentication value based in part on a sequence number indicating an ordinal position of a response request command in a sequence of response request commands.

As noted in the Office Action, the combination of Haverinen and Rofheart fails to disclose an expected value generation unit having the claimed features. In addition, Applicants respectfully traverse the assertion in the Office Action that Willey (paragraph [0072] and Fig. 11) discloses an expected value generation unit configured to generate an expected authentication value based on a sequence number that indicates a position of the response request command in a sequence of response request commands.²

Willey describes steps to "pair" via BLUETOOTH a device 200 and a device 1010, while preventing a "man-in-the-middle" attack.³ According to Willey, to overcome the man-in-the-middle attack, "both devices 200, 1010 perform a key agreement, and then each device

¹ Specification at page 26, lines 7-13.

² Office Action at page 5, lines 8-14.

³ Willey at paragraph [0070].

200, 1010 computes two separate antispooof variables 36 based on the shared secret (one for itself and one for the other device).”⁴ Furthermore, Willey indicates that a device 200 determines existence to the other device 1010 using a challenge including a random number with the same number of bits as the antispooof variable 36, and the random number acts as a challenge of the authenticated device 1010.⁵ In particular, Willey indicates that random numbers transmitted one bit at a time starting with the most significant bit and continuing with successively less significant bits and the authenticated device 1010 transmits a response to each portion of the challenge after receipt of the portion of the challenge.⁶ In addition, Willey indicates “[i]t is important that the function generates a response that varies both depending upon the received portion of the challenge and also depending upon the particular piece of information.”⁷ Thus, Willey indicates that each time a single bit of a random number is received, an authenticated device 1010 transmits a single bit of acknowledgement in response. Further, Willey indicates that the single bit of response “is the output of an exclusive or (XOR) function whose inputs are the just received bit of the random number and a bit of a device’s antispooof variable 36 (which may be one based upon its own address).”⁸

Thus, the response provided by Willey is a single bit produced by an XOR function between a random number and a variable based upon its own address. Thus, although Willey indicates that the bits vary depending upon the received portion of the challenge, Willey fails to indicate that any sequence number is generated by an expected value generation unit. Furthermore, Willey fails to indicate or suggest that any sequence number indicating an ordinal position (e.g., first, second, third, etc. . . .) of the response request command in sequence of response request commands is used to generate an expected authentication value.

⁴ Willey at paragraph [0071].

⁵ Willey at paragraph [0071].

⁶ Willey at paragraph [0071].

⁷ Willey at paragraph [0072].

⁸ Willey at paragraph [0072].

Willey merely indicates that an XOR function produces a single bit value. Accordingly, Applicants respectfully submit that Haverinen, Rofheart, and Willey fail to teach or suggest “an expected value generation unit configured to generate an expected authentication value based on the shared data and a sequence number, the sequence number indicating an ordinal position of the response request command in a sequence of response request commands to be transmitted by the command transmission unit,” as recited by Claim 1, and as similarly required by independent Claims 3, 4, 16, 18, 19, 21-23, and 26.

Therefore, Applicants respectfully submit that independent Claims 1, 3, 4, 16, 18, 19, 21-23, and 26, and claims depending therefrom, patentably define over Haverinen, Rofheart, and Willey.

Thus, it is respectfully requested the rejection of Claims 1-4, 16-19, 21-23, 25, and 26 under 35 U.S.C. § 103(a) be withdrawn.

In addition, Applicants respectfully traverse the rejection of Claims 6-14 under 35 U.S.C. § 103(a) as unpatentable over Haverinen and Rofheart.

Claim 6 is directed to a data receiving apparatus that includes, in part, a response message generation unit configured to generate a response message to a response request command before the response request command is received from a data transmitting apparatus.

Applicants respectfully submit that Haverinen and Rofheart fail to teach or suggest each of the features of independent Claims 6, 13, 14, and 25, and in addition, Applicants respectfully traverse the assertion in the Office Action that Haverinen (paragraphs [0170], [0177]-[0187], and [0211], and Fig. 2) discloses a response message generation unit that

generates a response message to a response request command *before* the response request command is received.⁹

Haverinen describes a communication between a foreign server FAAA and a home server HAAA.¹⁰ As shown in Haverinen Fig. 2, and as noted in the Office Action at page 13, Haverinen indicates that the SRES is already created at the MSC based on RAND before the MN RAND arrives at the GAGW. However, Applicants respectfully note that Figure 2 clearly indicates that a step of “Calculate SIGNrand = HMAC_MD5 (K, n*Kc+MN RAND)” is performed after the Registration Request is received by the PAC-GAGW. According to Haverinen, n*RAND, SIGNrand is transmitted in the registration reply to the MT. Thus, according to Haverinen, n*RAND, SIGNrand (e.g., a response message to a request command) is generated *after* the registration request command (e.g., “Request extension (NAI, MN RAND)”) is received, at least because SIGNrand is calculated based in part on MN RAND which is received in the registration request. Thus, even if the SRES is created at the MSC based on RAND, as asserted in the Office Action, Haverinen still fails to teach or suggest that a response message generation unit generates a response message to a response request command *before* the response request command is received. Rofheart also fails to teach or suggest the features lacking in Haverinen.

Accordingly, Applicants respectfully submit that Haverinen and Rofheart fail to teach or suggest “a response message generation unit configured to generate the response message to said response request command before said response request command is received from said data transmitting apparatus,” as recited in Claim 6, and as similarly required by independent Claims 13, 14, and 25.

⁹ Office Action at page 13, lines 2-16.

¹⁰ Haverinen at paragraph [0174].

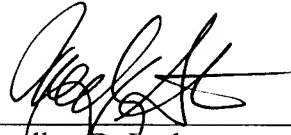
Therefore, it is respectfully submitted that independent Claims 6, 13, 14, and 25 patentably define over Haverinen and Rofheart, and accordingly, it is respectfully requested the rejection of Claims 6-14 under 35 U.S.C. § 103(a) also be withdrawn.

Accordingly, Applicants respectfully submit that independent Claims 1, 3, 4, 6, 13, 14, 16, 18, 19, 21-23, 25, and 26, and claims depending therefrom, are allowable.

Consequently, in light of the above discussion and in view of the present amendment, this application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 06/04)

Zachary S. Stern
Registration No. 54,719